National Infrastructure Protection Center
CyberNotes

Issue #2002-04 *February 25, 2002*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between February 2 and February 23, 2002. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Ada Core Technol-ogies[1]	Windows NT 4.0/2000, Unix	Gnat Pro Native 3.12p, 3.13p, 3.14p	A vulnerability exists in the runtime library of the GNU Ada compiler (Gnat) due to the way temporary files are handled, which could let a malicious user obtain root access.	No workaround or patch available at time of publishing.	Gnat Pro Native Insecure Temporary File	**High**	Bug discussed in newsgroups and websites.
Add2it[2]	Unix	Mailman Free 1.73	A vulnerability exists because user-supplied input to an 'open()' command is not properly filtered, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Mailman Free Arbitrary Command Execution	**High**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

[1] RUS-CERT Advisory, 2002-02:01, February 12, 2002.
[2] Securiteam, February 16, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Adobe[3]	Windows 95/98/ME/ NT 4.0/2000, XP	PhotoDeluxe 3.0, 3.1, 4.0	A vulnerability exists in the Java code that supports the "Connectables" feature, which could let an unauthorized malicious user obtain sensitive information and potentially execute arbitrary code.	No workaround or patch available at time of publishing.	PhotoDeluxe Java Applet	**Hgh**	Bug discussed in newsgroups and websites.
Alcatel[4]	Multiple	OmniPCX 4400	Multiple vulnerabilities exist: a vulnerability exists because system account passwords are known defaults, which could let remote malicious user obtain unauthorized access; a Denial of Service vulnerability exists because the shutdown utility on the system is installed with a setuid root bit; a vulnerability exists because shadowed passwords are not used, which could let a malicious user obtain elevated privileges; and a vulnerability exists because numerous files and directories are world readable, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	OmniPCX Multiple Vulnerabilities	Low/ Medium (Low if a DoS)	Bug discussed in newsgroups and websites. There is no exploit code required.
Apple[5]	MacOS 9x	MacOS 9.0, 9.0.4, 9.1, 9.2, 9.2.1, 9.2.2	A Denial of Service vulnerability exists if a reverse DNS lookup is being performed on a specific IP range.	No workaround or patch available at time of publishing.	MacOS 9 DNS Lookup Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Apple[6]	Windows 95/98/ME/ NT 4.0/2000, XP	QuickTime Player for Windows (Japanese) 5.0.1&5.0.2	A buffer overflow vulnerability exists due to insufficient bounds checking of the 'Content-Type' header, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	QuickTime Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Arescom[7]	Multiple	NET DSL 1000 Series ADSL Router	A remote Denial of Service vulnerability exists when a malicious user floods the Telnet configuration numerous times with long character strings.	No workaround or patch available at time of publishing.	NetDSL DSL ADSL Router Telnet Denial of Service	**High**	Bug discussed in newsgroups and websites.
Arescom[8]	Multiple	NetDSL 800U	A vulnerability exists due to the way administrative authentication is handled, which could let an unauthorized remote malicious user obtain administrative access to the router.	No workaround or patch available at time of publishing.	NetDSL DSL Router Administrative Authentication	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.

[3] Vulnerability Note, VU#116875, February 19, 2002.
[4] SecurityBugware Advisory, February 19, 2002.
[5] SecurityFocus, February 21, 2002.
[6] Shadow Penguin Security (SPS) Advisory #46, February 9, 2002.
[7] Bugtraq, February 8, 2002.
[8] Bugtraq, February 9, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Astaro[9]	Unix	Security Linux 2.016	Vulnerabilities exist due to improper file and directory permissions, which could let an unauthorized malicious user obscure their activity, perform a SSH man-in-the-middle attack, alter rpm checksums and potentially exploit the system with a Trojan rpm file, or other malicious activity.	Update available at: http://www.astaro.org/cgi/ultimatebb.cgi?ubb=get_topic&f=1&t=000095	Security Linux Multiple Vulnerabilities	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
BB Shareware. Com[10]	Windows 95/98/NT 4.0/2000	Phusion Webserver 1.0	Multiple vulnerabilities exist: a Directory Traversal vulnerability exists which could let a remote malicious user obtain sensitive information; a remote Denial of Service vulnerability exists when an unusually long URL is received; and a buffer overflow vulnerability exists when a long GET HTTP request is issued, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Phusion Webserver Multiple Vulnerabilities	Low/**High** **(Low for the DoS vulner-ability, and High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Blue World Communi-cations[11]	Windows NT	Lasso Web Data Engine 1.6.5	A vulnerability exists when an unusually long request is submitted to the Web Data Engine, which could let a remote malicious user crash the system.	No workaround or patch available at time of publishing.	Lasso Web Data Engine Overflow	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
BlueFace Software[12]	Windows	Falcon Web Server 2.0.0.1020, 2.0.0.1009	A vulnerability exists when a specially formed URL is requested, which could let a remote malicious user bypass authentication and view protected directories.	Upgrade available at: http://www.blueface.com/products.html#fws	Falcon Web Server Authentication Circumvention	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Caldera[13] ***Exploit scripts have been published.*** [14]	**Unix**	**UnixWare 7.1.1**	**A vulnerability exists in the library functions that are used to manipulate message catalogs, which could let a malicious user obtain elevated privileges.**	**Patch available at: ftp://stage.caldera.com/pub/security/unixware/CSSA-2002-SCO.3/erg711179.Z**	**UnixWare Library Function**	**Medium**	**Bug discussed in newsgroups and websites.** ***Exploit scripts have been published.***

[9] Bugtraq, February 12, 2002.
[10] Securiteam, February 17, 2002.
[11] Securiteam, February 18, 2002.
[12] Strumpf Noir Society Advisories, February 13, 2002.
[13] Caldera International, Inc. Security Advisory, CSSA-2002-SCO.3, February 7, 2002.
[14] Bugtraq, February 10, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Caldera International, Incorporated [15]	Unix	UnixWare 7.1.0, 7.1.1	The first version of this advisory stated that a vulnerability existed in the '/var/adm/isl/ifile' file because it is world readable and includes encrypted owner and root passwords, which could let a malicious user obtain sensitive information and elevated privileges. In the revised version Caldera has discovered files that are accessible to others that contain information that might be used to compromise the system's security.	**Workaround:** Caldera instructs administrators to change the mode of /var/adm/isl/ifile to be readable only by root: # chmod 400 /var/adm/isl/ifile They also suggest that the root and owner passwords be changed.	UnixWare Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Cisco Systems[16]	Multiple	Detailed list available at: http://www.cisco.com/warp/public/707/cisco-malformed-snmp-msgs-pub.shtml	A remote Denial of Service vulnerability exists when malformed SNMP packets are transmitted.	More detailed information and upgrade table is available at: http://www.cisco.com/warp/public/707/cisco-malformed-snmp-msgs-pub.shtml	IOS Malformed SNMP Message Denial of Service	Low	Bug discussed in newsgroups and websites.
Citrix[17]	Multiple	Nfuse 1.6	A vulnerability exists when the 'NFUSE_USER' and 'NFUSE_PASSWORD' parameters are submitted with arbitrary information, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	NFuse Network Sensitive Information	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Compaq Computer Corporation[18]	Multiple	Nonstop Kernel S-Series 3.0	A Denial of Service vulnerability exists due to a buffer overflow in the SNMP agent.	No workaround or patch available at time of publishing.	Nonstop Himalaya SNMP Agent Denial Of Service	Low	Bug discussed in newsgroups and websites.
Compaq Computer Corporation[19]	Multiple	TCP/IP Services For OpenVMS 5.3, Tru64 4.0g, 4.0f, 5.0a, 5.1a, 5.1	Several potential vulnerabilities exist in SNMPv1 trap handling and SNMPv1 Request handling, which could let a malicious user cause a Denial of Service or obtain unauthorized access.	No workaround or patch available at time of publishing.	Compaq SNMP Denial of Service	Low/ Medium (Medium if unauthorized access is obtained)	Bug discussed in newsgroups and websites.

[15] Caldera International, Inc. Security Advisory, CSSA-2002-SCO.5.1, February 16, 2002.
[16] Cisco Security Advisory, February 12, 2002.
[17] Bugtraq, February 20, 2002.
[18] Compaq Security Advisory, SSRT0799, February 18, 2002.
[19] Compaq Security Advisory, SSRT0799, February 18, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Coolsoft[20]	Windows 94/98/ME/ NT 4.0/2000, XP	PowerFTP 2.10 and prior	Multiple vulnerabilities exist: an information disclosure vulnerability exists because directory information is not properly parsed, which could let a malicious user obtain sensitive information; a vulnerability exists because FTP account information is stored unencrypted, which could let a malicious user obtain elevated privileges; Directory Traversal vulnerabilities exist because access to files outside of the user directory are not properly restricted, which could let a malicious user obtain sensitive information; and a Denial of Service vulnerability exists due to improper checking of the length of any of the arguments passed to the server.	No workaround or patch available at time of publishing.	PowerFTP Multiple Vulnerabilities	Low/ Medium **(Low for the DoS vulnera-bility; and Medium if sensitive informa-tion or elevated privileges are obtained)**	Bug discussed in newsgroups and websites. The Directory Traversal Vulnerabilities can be exploited via a web browser. The information disclosure vulnerability may be exploited with a FTP client
DCP-Portal [21]	Multiple	DCP-Portal 3.7, 4.0, 4.1, 4.2	A vulnerability exists when requests appended with 'add_user.php' are made to the host, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	DCP-Portal System Information Path Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
DCP-Portal[22]	Multiple	DCP-Portal 3.7, 4.0, 4.1, 4.2	A Cross-Site Scripting vulnerability exists which could let a remote malicious user execute arbitrary script commands.	No workaround or patch available at time of publishing.	DCP-Portal Cross Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Ettercap[23]	Unix	Ettercap 0.6.3.1	A buffer overflow vulnerability exists due to improper use of the 'memcpy()' function, which could let a remote malicious user execute arbitrary code as root.	Upgrade available at: http://ettercap.sourceforge.net /download/ettercap-0.6.4.tar.gz	Ettercap Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
EZNE.net[24]	Unix	Ezboard 1.27	A remote buffer overflow vulnerability exists in some of the CGI programs, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Ezboard Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[20] Strumpf Noir Society Advisories, February 11, 2002.
[21] ALPER Research Labs Security Advisory, ARL02-A02, February 15, 2002.
[22] ALPER Research Labs Security Advisory, ARL02-A03, February 15, 2002.
[23] Next Generation Security Technologies Security Advisory, NGSEC-2002-1, February 5, 2002.
[24] Securiteam, February 12, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Funsoft[25]	Windows 95/98/ME	Dino's Webserver 1.0, 1.2	A Denial of Service vulnerability exists when a malicious user submits multiple GET requests with an unusually long string of characters.	No workaround or patch available at time of publishing.	Dino's Webserver Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Gator[26]	Windows	Gator 3.0.6.0	A vulnerability exists in a plugin that installs the Gator software, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Gator Insecure Plugin	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
GNUJSP[27]	Windows NT 4.0/2000, Unix	GNUJSP 1.0.0, 1.0.1	A vulnerability exists in a Java servlet that allows you to insert Java source code into HTML files, which could let a remote malicious user obtain sensitive information.	**Debian:** http://security.debian.org/dists/stable/updates/contrib/binary-all/gnujsp_1.0.0-5_all.deb	GNUJSP File Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Hewlett Packard Company[28]	Unix	HP-UX 11.11	A Denial of Service vulnerability exists because arguments are incorrectly specified for the 'setrlimit()' function.	Patch available at: http://itrc.hp.com PHKL_26233	HP-UX 'strlimit()' Denial of Service	Low	Bug discussed in newsgroups and websites.
Hewlett Packard Systems[29]	Multiple	Advance Stack 10Base-T Switching Hub J3210A	A vulnerability exists which could let an unauthorized malicious user bypass authentication restrictions and obtain administrative access.	See HP Security Advisory workaround available at: ftp.itrc.hp.com:~ftp/export/patches/hp-ux_patch_matrix	AdvanceStack Authentication Bypass	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Hewlett Packard Systems[30]	Multiple	JetDirect x.08.32	A Denial of Service vulnerability exists if the printer receives a malformed SNMP packet.	No workaround or patch available at time of publishing.	JetDirect SNMP Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
HNS[31]	Unix	HNS 2.00-pl0-2.00-pl4, 2.10-pl1, hns-lite 0.6-0.8	Cross-site scripting vulnerabilities exist in the 'log.cgi' and 'title.cgi' scripts, which could let a malicious user execute arbitrary script code.	Update available at: http://www.h14m.org/dist/	HNS Multiple Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites.
Identix[32]	Windows NT 4.0/2000, XP	BioLogon 3.0	A vulnerability exists in the GINA (Graphical Identification and Authentication) interface, which could let a malicious user gain system privileges.	Contact the vendor regarding the patch at: idxsupport@identix.com	BioLogon GINA Authentication Bypass	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.

[25] Bugtraq, February 18, 2002.
[26] Vulnwatch, February 20, 2002.
[27] Debian Security Advisory, DSA 114-1, February 21, 2002.
[28] Hewlett-Packard Company Security Advisory, HPSBUX0202-183, February 12, 2002.
[29] Hewlett-Packard Company Security Advisory, HPSBUX0202-185, February 12, 2002.
[30] Bugtraq, February 19, 2002.
[31] HyperNikkiSystem Project, hns-SA-2002-01, February 14, 2002.
[32] Securiteam February 15, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Instant Servers[33]	Windows	MiniPortal 1.1.5	Multiple vulnerabilities exist: a vulnerability exists because account information and login and session data are stored in plaintext, which could let a malicious user obtain elevated privileges; a Directory Traversal vulnerability exists because access to files outside of the user directory are not properly restricted, which could let a malicious user obtain sensitive information; and a remote buffer overflow vulnerability exists due to improper bounds checking in the logging routine, which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.instantservers.net/download/minip116.zip	MiniPortal Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required for the Directory Traversal, and plaintext account and login vulnerabilities.
Internet Security Systems[34] ***Further research released.[35]***	**Windows 2000, XP**	**BlackIce Agent 3.0, 3.1, BlackICE Defender 2.9caq, 2.9cap; RealSecure Server Sensor 6.0.1 Win, 6.5 Win**	**A remote Denial of Service vulnerability exists when a continuous series of ICMP Echo Request 10,000 byte packets are sent to the server.** ***Further research indicates that this is a remote buffer overflow vulnerability, which allows the execution of arbitrary code.***	***Patch available at:*** http://www.iss.net/support/consumer/BI_downloads.php	***BlackICE and RealSecure Denial of Service and Buffer Overflow***	**Low/High** ***(High if DDoS best practices not in place and arbitrary code can be executed.)***	**Bug discussed in newsgroups and websites. There is no exploit code required.** **Vulnerability has appeared in the press and other public media.**
Lotus[36]	Windows NT 4.0/2000, OS/2 4.5Warp, OS/390 V2R9, Unix	Domino 5.0-5.0.8	A vulnerability exists if an HTTP request is submitted for a non-existent .pl file, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Domino Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Microsoft[37]	Windows 2000	Windows 2000 Server, 2000 Server SP1& SP2	A vulnerability exists because the terminal will not lock after a disconnect via the Terminal Services client, which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	Windows 2000 Server Terminal Services Terminal Lock	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[33] Strumpf Noir Society (SNS) Advisories, February 9, 2002.
[34] Internet Security Systems Security Alert, ISS-109, February 4, 2002.
[35] eEye Digital Security Alert, February 8, 2002.
[36] KPMG-2002004, February 4, 2002.
[37] NTBugtraq, February 11, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Microsoft[38]	Windows 2000	Commerce Server 2000	A vulnerability exists because AuthFilter contains an unchecked buffer in a section of code that handles certain types of authentication requests, which could let a malicious user execute arbitrary code and take complete control over the web server.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-010.asp	Commerce Server 2000 ISAPI Buffer Overflow CVE Name: CAN-2002-0050	**High**	Bug discussed in newsgroups and websites.
Microsoft[39]	Windows 95/98/ME/ NT 4.0/2000	Internet Explorer 5.01, 5.01SP1&2, 5.5, 5.5SP1&2, 6.0	Six vulnerabilities exist: a buffer overflow vulnerability exists when a specially formed web page is created and either posted or sent to a user as an HTML mail, which could let a malicious user execute arbitrary code; a vulnerability exists because the 'GetObject' function's security checks can be spoofed, which could let a malicious user obtain sensitive information; a vulnerability exists because HTML header information in a web page can me manipulated in order to make the IE File Download dialogue display the wrong file name and type, which could let a malicious user fool a user into downloading an unsafe file; a vulnerability exists because of a flaw in the way IE processes the Content-Type HTML header field, which could let a malicious user execute an arbitrary file; a vulnerability exists because of a flaw associated with an HTML directive that allows events to occur asynchronously on a web page, which could let a malicious user bypass the user's security settings and run script even if scripting has been disabled; and a newly discovered variant of the "Frame Domain Verification" vulnerability (discussed in Microsoft Security Bulletin MS01-058) exists in the 'Document.open' function , which could let a malicious user obtain sensitive information.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-005.asp	Internet Explorer Multiple Vulnerabilities CVE Names: CAN-2002-0022, CAN-2002-0023, CAN-2002-0024, CAN-2002-0025, CAN-2002-0026, CAN-2002-0027	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.

[38] Microsoft Security Bulletin, MS02-010, February 21, 2002.
[39] Microsoft Security Bulletin, MS02-005, February 11, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Microsoft[40]	Windows 95/98/ME/ NT 4.0/2000	Internet Explorer 5.01, 5.01SP1&2, 5.5, 5.5SP1&2, 6.0	A vulnerability exists in the way VBScript is handled in IE relating to validating cross-domain access, which could let a malicious user obtain sensitive information.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-009.asp	Internet Explorer VBScript Policy Violation CVE Name: CAN-2002-0052	Medium	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Microsoft[41]	Windows 95/98/ME/ NT 4.0/2000	Outlook Express 5.5, 6.0	A vulnerability exists when the subject line of an e-mail message contains carriage returns, which could let a malicious user send an arbitrary attachment.	No workaround or patch available at time of publishing.	Outlook Express Non-existing Attachment	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Microsoft[42]	Windows 95/98/NT 4.0/2000, XP	Windows 95, 98, 98SE, NT 4.0, NT 4.0 Server, Terminal Server Edition, 2000, XP	A buffer overflow vulnerability exists because the component of the SNMP agent service that parses incoming commands contains an unchecked buffer, which could let a malicious user cause a Denial of Service or execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-006.asp	Windows Unchecked Buffer SNMP Service CVE Name: CAN-2002-0053	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Microsoft[43]	Windows NT 4.0	SQL Server 7.0 SP1-3 alpha, 7.0 SP1-3, 2000, 2000SP1-3	A buffer overflow vulnerability exists due to the way OLD DB provider names are handled in ad hoc connections, which could let a remote malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-007.asp	SQL Server OLE DB Provider Name Buffer Overflow CVE Name: CAN-2002-0056	**High**	Bug discussed in newsgroups and websites.
Microsoft[44]	Windows XP	Microsoft XML Core Services versions 2.6, 3.0, and 4.0	A vulnerability exists in how the XMLHTTP control applies IE security zone settings to a redirected data stream, which could let a malicious user obtain sensitive information.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-008.asp	Windows XP XMLHTTP Sensitive Information CVE Name: CAN-2002-0057	Medium	Bug discussed in newsgroups and websites.
Multiple Vendors[45]	Windows 95/98/ME/ NT 4.0/2000, MacOS 8.0/ 8.1/ 8.5.8.6/9.0, Unix	Multiple Vendors (for complete list, see: http://online.securityfocus.com/bid/4131	A vulnerability exists in software and integrated server packages that function as web proxies through the HTTP Connect method, which could let a remote malicious user launch attacks against internal machines.	No workaround or patch available at time of publishing.	Multiple Vendor HTTP CONNECT TCP Tunnel	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[40] Microsoft Security Bulletin, MS02-009, February 21, 2001.
[41] Bugtraq, February 12, 2002.
[42] Microsoft Security Bulletin, MS02-006, February 15, 2002.
[43] Microsoft Security Bulletin, MS02-007, February 21, 2002.
[44] Microsoft Security Bulletin, MS02-008, February 21, 2002.
[45] SecurityFocus, February 23, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Multiple Vendors[46]	Windows 95/98/ME/ NT 4.0/2000, Unix	3com Dual-Speed, PS & Hub, Switch, WebCache; AdventNet Agent Tool-kit, CLI API, Management Toolkits & Builder, Mediation, SNMP, Web NMS; CacheFlow; Caldera OpenServer, UnixWare; CA Unicenter; Comtek Services NMServer; HP EMS, UX, (VVOS), JetDirect, Service Guard, MPE/iX, OpenView, Procurve Switch; Innerdive Solutions IP Console; Juniper Networks JUNOS 5.0; Lantronix; Domino SNMP Agents; Windows, XP; Net-SNMP ucd-snmp; Netware; Process Software; RedBack Networks; SNMP Research; Sun Solaris	Multiple vulnerabilities exist in several SNMP implementations in the process of decoding and interpreting SNMP trap messages. These vulnerabilities may cause Denial of Service conditions, service interruptions, and in some cases may allow a malicious user to gain access to the affected device. Specific impacts will vary from product to product. *Note: For more detailed information, see* CERT® Advisory CA-2002-03, located at: http://www.cert.org/advisories/CA-2002-03.html.	Contact your vendor for patch or see CERT Advisory located at: http://www.cert.org/advisories/CA-2002-03.html	Multiple Vendor SNMP Trap Handling CVE Name: CAN-2002-0012	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.

[46] CERT® Advisory CA-2002-03, February 12, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Multiple Vendors[47]	Windows 95/98/ME/ NT 4.0/2000, XP	FastTrack KaZaA 1.2-1.5; Grokster Grokster 1.3, 1.3.3; Music City Networks Morpheus 1.3, 1.3.3	A vulnerability exists because access control is based on client identities in request headers, which could let a malicious user spoof the identity of a valid user.	No workaround or patch available at time of publishing.	Multiple Vendor Identity Spoofing	Low/ Medium (Low for the DoS)	Bug discussed in newsgroups and websites. Exploit has been published.
Multiple Vendors[48]	Windows 95/98/ME/ NT 4.0/2000, XP	FastTrack KaZaA 1.2-1.5; Grokster Grokster 1.3, 1.3.3; Music City Networks Morpheus 1.3, 1.3.3	A Denial of Service vulnerability exists when a malicious user sends messages repeatedly.	**FastTrack KaZaA:** http://www.kazaa.com/en/index.htm	FastTrack P2P Technology Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Multiple Vendors[49, 50]	Unix	Easy Software Products CUPS 1.0.4, 1.1.7, 1.1.10, 1.1.13	A buffer overflow vulnerability exists when the names of attributes are read, which could let a remote malicious user execute arbitrary code.	**Debian:** http://security.debian.org/dists/stable/updates/main/ **MandrakeSoft:** http://telia.dl.sourceforge.net/mirrors/mandrake/updates/	Multiple Vendor CUPS Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Netgear[51]	Multiple	Netgear RM-356, RT-338	A remote Denial of Service vulnerability exists when portscanning the router with UDP.	**Workaround**: Connect to the device via Telnet. Forward the 'Default' address in Menu 15 [default is 0.0.0.0] to a non-existent IP address (for example: 192.168.0.99 for instance) on your LAN, then port scans would be forwarded to 'nowhere'.	Netgear Denial Of Service	Low	Bug discussed in newsgroups and websites. This vulnerability may be exploited with publicly available tools.
NetWin[52]	Multiple	WebNEWS 1.1j, 1.1I, 1.1h	A buffer overflow vulnerability exists when an unusually long value is supplied as a group parameter, which could let a remote malicious user execute arbitrary code.	Upgrade available at: ftp://ftp.netwinsite.com/pub/webnews/webnews11k.exe	WebNEWS Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
NetWin[53]	Multiple	WebNEWS 1.1k, 1.1j, 1.1I, 1.1h	A vulnerability exists because several default accounts have been hard-coded, which could let a remote malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	WebNEWS Hard-Coded Programs	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[47] SecurityFocus, February 19, 2002.
[48] SecurityFocus, February 19, 2002.
[49] Debian Security Advisor, DSA 110-1, February 13, 2002.
[50] Mandrake Linux Security Update Advisory, MDKSA-2002:015, February 15, 2002.
[51] Bugtraq, February 15, 2002.
[52] NGSSoftware Insight Security Research Advisory, NISR18022002, February 19, 2002.
[53] Bugtraq, February 21, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
NetWin Limited[54]	Windows 95/98/NT 4.0/2000, MacOS X 10.0, Unix	CWMail 2.7, 2.7a-2.7d, 2.7f, 2.7i-2.7q, 2.7s, 2.7t	A buffer overflow vulnerability exists when the 'item=' is filled with a large string of characters, which could let a malicious user execute arbitrary code.	Upgrade available at: http://netwinsite.com/dmailweb/download.htm	CWMail.exe Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Nombas[55]	Windows, OS/2, Unix	ScriptEase: Webserver Edition 0.95 win3.x, Solaris, ppc, OS/2, Netware 5, Linux, ISAPI win32, Irix, HP-UX, FreeBSD, CGIWINCGI win32	Multiple Denial of Service vulnerabilities exist when a malicious user submits a request that is composed of an unusual number of arbitrary character sequences.	No workaround or patch available at time of publishing.	SriptEase:Web Server Edition Multiple Denial of Service Vulnerabilities	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Novell[56]	Windows	Groupwise 6.0	A vulnerability exists when a system is configured to use LDAP authentication and the password filed is left blank, which could let a malicious user bypass authentication.	Patch available at: http://support.novell.com/	GroupWise LDAP Authentication Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Opera Software[57]	Windows 95/98/ME/ NT 4.0/2000, XP	Opera Web Browser 6.0.1win32	A vulnerability exists because files based on the Content-Type header of an HTTP object are not properly handled, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	Opera Content-Type HTML File Execution	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
PHP Development Team[58]	Multiple	PHP 4.0, 4.0.1pl2, 4.0.1, 4.0.3-4.0.6. 4.1, 4.1.1	A vulnerability exists in the default configuration when PHP or JSP 'include' files are kept in the same directory as the file calling them, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	PHP or JSP Include File Sensitive Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Powie[59]	Unix	PForum 1.14	A vulnerability exists if the "Magic Quotes" option in PHP is disabled which could let an unauthorized malicious user log in as administrator without any authentication.	**Temporary workaround:** PHP has a configuration option titled "MagicQuotes ." It can be enabled in php.ini with the "magic_quotes_gpc" setting. This filters quote injection attempts.	PForum User Authentication	**High**	Bug discussed in newsgroups and websites.

[54] NGSSoftware Insight Security Research Advisory, NISR12022002, February 13, 2002.
[55] Bugtraq, February 19, 2002.
[56] Bugtraq, February 20, 2002.
[57] Geekgang Security Advisory, GSA2002-01, February 12, 2002.
[58] Advisory #3, February 7, 2002.
[59] Securiteam, February 18, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Prospero Technol-ogies [60]	Multiple	Message Boards	A Cross-Site Scripting vulnerability exists because posted HTML formatted messages may contain JavaScript commands, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Message Board Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Sawmill[61]	Unix	Sawmill 6.2-6.2.14	A vulnerability exists because the 'AdminPassword' file is created with insecure default permissions on Solaris platforms, which could let a malicious user obtain unauthorized access.	Upgrade available at: http://www.sawmill.net/downloads.html	Sawmill Admin Password Insecure Default Permissions	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Sitenews[62]	Windows NT 4.0/2000, Unix	Sitenews 0.01 beta-0.11 beta	A vulnerability exists when a non-existent username is requested, which could let an unauthorized remote malicious add users to the database and take full control over all news items and users.	Upgrade available at: http://www.linuxnetwork.nl/download.php?what=download&dl_id=38	Sitenews Unauthorized Control	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Slashcode[63]	Unix	Slashcode 1.0.8 and previous, 2.0-2.2.4	A Cross-Site Scripting vulnerability exists when users who have JavaScript enabled are persuaded to click on a malicious URL, which could let a malicious user execute arbitrary script commands.	Upgrade available at: http://prdownloads.sourceforge.net/slashcode/slash-2.2.5.tar.gz	SlashCode Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites.
Stefan Holmberg[64]	Multiple	AdMentor 2.11	A vulnerability exists if special characters are included in the login parameters, which could let an unauthorized remote malicious user login as admin.	No workaround or patch available at time of publishing.	AdMentor Remote Login	**High**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser..
Sun Micro-systems[65]	Unix	Solaris 2.5.1, 2.5.1_x86& ppc, 2.6sparc, 2.6HW5/98, 2.6HW3/98, 2.6_x86HW 5/98, 2.6_x86HW 3/98, 2.6_x86, 2.6, 7.0_x86, 7.0_x86, 0, 8.0_x86, 8.0	A vulnerability exists involving the interaction of mail and sendmail when mail is invoked from a privileged program, which could let an unauthorized local or remote malicious user obtain elevated privileges and execute arbitrary code as the root user.	Patch available at: http://sunsolve.sun.com	Solaris Mail Command Execution	**High**	Bug discussed in newsgroups and websites.

[60] CERT Advisory, CA-2000-02, February 2, 2002.
[61] Warped Force Advisory #2, February 11, 2002.
[62] Bugtraq, February 16, 2002.
[63] SA-2002:01, February 19, 2002.
[64] Bugtraq, February 21, 2002.
[65] SecurityFocus, February 14, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Sybex[66]	Windows 94/98/NT 4.0/2000	E-Trainer	A Directory Traversal vulnerability exists because user input is not properly sanitized, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	E-Trainer Directory Traversal	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Symantec[67]	Windows NT 4.0/2000	Enterprise Firewall 6.5.2 NT/2000	Several vulnerabilities exist: a vulnerability exists in the SMTP header when connections are mapped using NAT (Network Address Translation), which could let a malicious user obtain sensitive information; and a vulnerability exists because the SNMP reporting mechanism fails to forward messages, which could let a remote malicious attack against the firewall go undetected.	**Workaround:** SMTP Header vulnerability: Configure Symantec Enterprise Firewall to use the same name for the firewall name and the firewall external interface name. This workaround results in consistent names for SMTP replies. If NAT is not needed, use the SMTP wizard included with Symantec Enterprise Firewall to set up rules and redirects for all inbound and outbound SMTP traffic.	Enterprise Firewall SMTP Proxy Information Leak and Firewall Notify Daemon SNMP Data Loss	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Tarantella[68]	Unix	Enterprise 3 3.0, 3.0, 3.10, 3.11, 3.20	A symbolic link vulnerability exists in the installation process, which could let a malicious user obtain elevated privileges including root.	No workaround or patch available at time of publishing.	Enterprise 3 Symbolic Link	**High**	Bug discussed in newsgroups and websites.
University of Cambridge[69]	Unix	Exim 3.34	A buffer overflow vulnerability exists when a combination of flags is executed, which could let a malicious user obtain elevated privileges.	Update available at: ftp://ftp.csx.cam.ac.uk/pub/software/email/exim/exim3/exim-3.35.tar.gz	Exim Buffer Overflow	Medium	Bug discussed in newsgroups and websites.
USANet Creations[70]	Unix	MakeBid Auction Deluxe 3.30	Multiple vulnerabilities exist: a vulnerability exists because login credentials are stored in plaintext in a cookie, which could let a malicious user obtain sensitive information; and a Cross-Site Scripting vulnerability exists because script code is not properly filtered from form fields, which could let a malicious user execute arbitrary code.	Patch available for the Cross-Site Scripting vulnerability at: http://www.netcreations.addr.com/updates/index.html There is no workaround or patch available at time of publishing for the plaintext login vulnerability.	MakeBid Auction Plaintext Login and Cross-Site Scripting	Medium **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.

[66] Bugtraq, February 9, 2002.
[67] Corsaire Limited Security Advisory, February 20, 2002.
[68] Bugtraq, February 19, 2000.
[69] SecurityFocus, February 21, 2002.
[70] Securiteam, February 15, 2002.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. *DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.*

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between February 5 and February 21, 2002, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 25 scripts, programs, and net-news messages containing holes or exploits were identified. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

February 21, 2002	Ucd-421.c	Script which exploits the UCD-snmp Trap Handling vulnerability.
February 18, 2002	Agate.c	Script which exploits the Avirt Gateway 4.2 remote vulnerability.
February 18, 2002	Dhb.zip	Tool that tries to guess Lotus Domino HTTP passwords.
February 18, 2002	Ettercap-0.6.3.txt	Technique for exploiting the Ettercap Buffer Overflow vulnerability.
February 18, 2002	Ettercap-0.6.4.tar.gz	A network sniffer/interceptor/logger for switched LANs that uses ARP poisoning and the man-in-the-middle technique to sniff all the connections between two hosts.
February 18, 2002	Mimedefang-2.5.tar.gz	MIME e-mail scanner designed to protect Windows clients from viruses and other harmful executables.
February 18, 2002	Nsat-1.41.tar.gz	A fast, stable bulk security scanner designed to audit remote network services and check for versions, security problems, gather information about the servers and the machine and much more.
February 18, 2002	**Phusion-web.txt**	**Exploit information for the Phusion Webserver Multiple Vulnerabilities.**
February 18, 2002	Rats-1.3_win32_bin.zip	A security auditing utility for C, C++, Python, Perl and PHP code.
February 18, 2002	**Snscan.zip**	**a Windows GUI SNMP detection utility that can quickly and accurately identify SNMP enabled devices on a network. This utility can effectively indicate devices that are potentially vulnerable to SNMP related security threats**
February 17, 2002	**Phusion_dos.pl**	**Exploit for the Phusion Webserver Multiple Vulnerabilities.**
February 17, 2002	**Phusion_exp.pl**	**Exploit for the Phusion Webserver Multiple Vulnerabilities.**

February 17, 2002	**Phusion-get.pl**	**Exploit for the Phusion Webserver Multiple Vulnerabilities.**
February 17, 2002	**Phusion-ovrun.c**	**Exploit for the Phusion Webserver Multiple Vulnerabilities.**
February 12, 2002	**Ez2crazy.pl**	**Perl script which exploits the Ezboard 2000 Remote Buffer Overflow vulnerability.**
February 11, 2002	Lkh-1.1-linux-2.4.10.tgz	A powerful and documented kernel function hooking library running on Linux 2.4/x86 that has been explained and the API described in Phrack #58.
February 11, 2002	Mircexploit-V591.c	Proof of concept exploit for the buffer overflow vulnerability that exists in the nick handling code of mIRC.
February 11, 2002	**Morpheus.c**	**Exploit for the FastTrack P2P Technology Identity Spoofing and Denial of Service vulnerability.**
February 11, 2002	Silentlog.zip	A keystroke logging tool that runs under several Windows 32 versions (it should also run under NT).
February 11, 2002	Snexploit	Exploit for a buffer overflow vulnerability in the snes9x Nintendo emulator.
February 9, 2002	**Applequicktimeexploit.c**	**Exploit for the QuickTime Remote Buffer Overflow vulnerability.**
February 7, 2002	Expshell.c	Script which exploits the UnixWare Library Function vulnerability.
February 7, 2002	Fmt_exp.c	Script which exploits the UnixWare Library Function vulnerability.
February 7, 2002	Getret.c	Script which exploits the UnixWare Library Function vulnerability.
February 5, 2002	Ettercap-X.c	Ettercap Buffer Overflow vulnerability.

Trends

- **The National Infrastructure Protection Center is aware of potential vulnerabilities existing within the Simple Network Management Protocol (SNMP) -- a protocol used by routers, switches and hubs on the Internet and other related equipment. For more information, see NIPC ALERT 02-001, located at: http://www.nipc.gov/warnings/alerts/2002/02-001.htm.**
- **Numerous vulnerabilities have been reported in multiple vendors' SNMP implementations. For more information, see CERT® Advisory CA-2002-03, located at: http://www.cert.org/advisories/CA-2002-03.html.**
- **The National Infrastructure Protection Center (NIPC) has received reporting that infrastructure related information, available on the Internet, is being accessed from sites around the world. While in and of itself this information is not significant, it highlights a potential vulnerability. For more information, see NIPC ADVISORY 02-001, located at: http://www.nipc.gov/warnings/advisories/2002/02-001.htm.**
- **The CERT/CC has received credible reports of scanning and exploitation of Solaris systems running the CDE Subprocess Control Service buffer overflow vulnerability identified in CA-2001-31 and discussed in VU#172583. For more information, see CERT® Advisory CA-2002-01, located at: http://www.cert.org/advisories/CA-2002-01.html.**
- **NIPC has updated their advisory, NIPC Advisory 01-030, regarding what Microsoft refers to as a critical vulnerability in the universal plug and play (UPnP) service in Windows. For more information see, NIPC ADVISORY 01-030.3, located at: www.nipc.gov/warnings/advisories/2001/01-030-2.htm.**

Viruses

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication**. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available**. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found. During this month, a number of anti-virus vendors have included information on Trojan Horses and Worms. Following this table are descriptions of new viruses and updated versions discovered in the last two weeks. NOTE: At times, viruses may contain names or content that may be considered offensive.

	Common Name			
1	W32/SirCam.A	Worm	Slight Increase	July 2001
2	W32/BadTrans.B	Worm	Slight Decrease	April 2001
3	W32/Nimda.A	File, Worm	Stable	September 2001
4	W32/MyParty.A	File, Worm	New to Table	January 2002
5	W32/Hybris.B	File, Worm	Slight Decrease	November 2000
6	W32/Magistr.A	File, Worm	Stable	March 2001
7	W32/Magistr.A	File, Worm	Stable	March 2001
8	W32/Klez.E	Worm	New to Table	January 2002
9	W32/Nimda.D	File, Worm	Slight Decrease	September 2001
10	W32/Funlove.4099	File	Slight Decrease	November 1999

Note: Virus reporting may be weeks behind the first discovery of infection. A total of **201** distinct viruses are currently considered "in the wild" by anti-virus experts, with another **463** viruses suspected. "In the wild" viruses have been reported to anti-virus vendors by their clients and have infected user machines. The additional suspected number is derived from reports by a single source.

IRC.Worm.Ceyda (Aliases: IRC-Worm.Ceyda.6574, mIRC/Ceydem.6953/6966, pIRCH/Ceydem.6966) (IRC Worm): This is an IRC worm that sends itself to others using IRC. It allows a malicious user to gain control of an infected system. This worm is an encrypted DOS executable file. When it is executed, it does the following:

- First, it decrypts itself
- It then creates the Winstart.bat file in the C:\Windows folder
- Next, it creates the C:\Windows\Windowsuser2 folder, and copies itself to that location
- It then executes the batch file. The batch file makes another copy of the worm in the \Windowsuser2 folder with the file name CeydaDemet___TurkishGirl.JPG.com
- It also creates a Script.ini file in the C:\Mirc folder. The worm replaces certain commands in the Script.ini with commands to format the hard drive and to send itself to others.

JS/Coolnow-A (Alias: JS.Menger.worm) (JavaScript Worm): This is an MSN Messenger worm which exploits a vulnerability in Microsoft Internet Explorer. The body of the worm exists on a web page. When a vulnerable user views the page, the worm will send a message to all the user's MSN Messenger contacts.

The message will ask the recipient to visit the affected web page. The text of the message will vary according to the affected web page but may be similar to "Go to: http://<address of affected website>." The worm makes no modifications to a user's system. Microsoft has issued a security patch, which secures against the vulnerability. It is available from http://www.microsoft.com/technet/security/bulletin/ms02-005.asp.

VBS/Numgame-A (Alias: GuessGame) (Visual Basic Script Worm): This is an e-mail worm. When the attachment, "GuessGame.html," is run it will display a message box containing the text "Guess Game instructions:" and asking the user to click Yes when an ActiveX dialog box appears. Depending on the system configuration, an ActiveX warning dialog may then be displayed. If the user clicks Yes to the ActiveX warning, or no warning appears, the worm will create the file GuessGame.vbe in the Windows directory and execute it. GuessGame.vbe will first create a copy of itself in the Windows system directory and then send an e-mail to all addresses listed in the user's Outlook Address book. It will next attempt to set the date to 04-08-1981. Depending on the system settings, this will result in the system date changing to 4th August 1981 or 8th April 1981 or re-mailing unchanged. It will also set the following registry values in order to disable the Desktop and the system file checking process.

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SFCDisable = 0xFFFFFF9D

HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDesktop = 1

After setting the registry entries, the worm will attempt to delete all files from the local and network drives. On each affected drive it will also create a file named autoexec.bat in an attempt to delete files with the following extensions: .SYS, .DLL, .OCX, .CPL, .DAT, .COM, .EXE, .CAB, .INI, .INF, .VXD, .DRV, .DOC, .XLS, .MDB, .PPT, .MP3, .JPG, .TXT, .HTM, .HTML, .HTA, .ASP, .ASPX, from the following directories:

- Desktop
- Program Files
- My Documents
- Windows
- System
- Temp
- Windows\SYSTEM32
- Windows\COMMAND
- Windows\INF
- Windows\SYSBCKUP
- \Documents and Settings
- \Inetpub

or their equivalents (e.g. WINNT\system32). Next, the worm will allow the user to play a guessing game to guess a number between 1 and 100.

W32/Admirer@MM (Win32 Worm): This mass-mailing worm poses as a Macromedia Flash movie. It arrives in an e-mail message with the attachment, ValentineCard.exe. Executing the attachment infects the local machine. The worm copies itself to the WINDOWS SYSTEM directory as ValentineCard.exe and creates a registry run key to load itself at startup.

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\
Run 14th=C:\WINDOWS\SYSTEM\ValentineCard.exe

It sends itself to all users found in the Microsoft Outlook Address Book using MAPI messaging. A registry key is created for the worm to note that it has run before.

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\
Valentine=true

After the first run, the worm creates a WAV file, C:\EVIL.JPG, and opens it. As the file contains the incorrect extension, the file does not open properly.

W32/Alcarys@MM (Win32 Worm): This is a multifaceted worm. It contains many components and uses different methods to carry out its payloads. It arrives in an e-mail message and the following attachments:

- ? sexsounds.wav (SexSound.exe)
- ? and haiku for you (readme.txt)
- ? and http://www.EcstasyRUs.com (www.EcstasyRUs.com)
- ? and the cool talking screensaver (syra.scr)

Except for the haiku text file, the attachments are all identical copies of the same worm with a different filename. When any of the other attachments are run, this worm infects the local system. The worms sends itself to all users found in the Microsoft Outtlook address book using MAPI messaging.

W32.Alcarys.B@mm (Win32 Worm): This is a mass mailing worm that will send to all recipients in an affected user's address book. It will also stall the machine such that the machine will only be usable once it is started in MS-DOS mode. It will also overwrite many System files.

W32/Bezilom.worm (Win32 Worm): This worm (written in Visual Basic 6) arrives in the form of a dropper and is multi-component in nature. When executed the dropper displays a pornographic image (JPG), as well as installing and executing the other worm components:

- ? MARIA.DOC, multiple spaces .EXE - Trojan to simulate infected machine
- ? MACROSOFTBT.EXE - fake anti-virus scanner

When executed, MARIA.DOC.EXE copies itself to the root of C: with a random name (hidden file attribute set), and also to %windir% as MARIA.DOC.EXE. It overwrites AUTOEXEC.BAT with a single line pointing to C:\random name.exe. This process is repeated at each bootup, leading to an accumulation of copies of the worm. The following Registry key is set to ensure the worm is run at system startup:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows_
\CurrentVersion\Run "Startup" = %windir%\MARIA.DOC.EXE

When the second component is run, it creates the (hidden) directory 'MacrosoftBL' in the 'Program Files' directory, and copies itself there (as MACROSOFTBL.EXE, hidden file attributes). The following Registry key is set to ensure the fake anti-virus scanner is executed at system startup:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows_
\CurrentVersion\Run "Macrosoft" = c:\program files_MacrosoftBL\MACROSOFTBL.EXE

Upon rebooting, both components are active in memory. After a number of reboots, MARIA.DOC.EXE causes all launched windows to be hidden (except MacrosoftBL windows), in order to mimick a virus infection. The second component, MacrosoftBL, then triggers a virus infection. Following the link to registration details, a form detailing how to pay is displayed.

W32.HLLO.6144 (Win32 Virus): This virus is written in a high-level language. When it is executed, it searches for all .com, exe, and .scr files in all folders on the hard drive. It then replaces these files with an exact copy of itself. The replaced program files are not repairable.

W32/Rexli-A (Win32 Worm): This is an e-mail worm. When the worm is first executed, it will display a fake error message with the text "Error while loading <filename>", where <filename> will normally be linki.exe. Next, it will attempt to e-mail a copy of itself to all addresses in the user's Outlook address book. The worm creates copies of itself named, linki.exe and rexec.exe, in the Windows system directory and replaces any .VBS files on the hard disk with a script, which will attempt to run the worm. W32/Rexli-A also uses mIRC to spread. It will replace the mIRC script.ini file with one that will send a copy of the worm to other IRC users. The new script.ini file will be detected by SAV as mIRC/Simp-Fam. A count of the number of times the worm has been run is kept in the registry key:

HKCU\Software\VB and VBA Program Settings\Rax\General\Runs

When this number reaches 100, the worm will delete the files himem.sys, ifshlp.sys, and win.com from the Windows directory and himem.sys from the Windows command\ebd directory. It will also modify autoexec.bat so that the next time the computer is booted the file internat.exe in the Windows directory will be renamed to internat.bak and replaced with a copy of the worm.

W32.HLLO.Rozak (W32 Virus): This is a virus that overwrites .exe, .mpg, .mpg4, .zip, .doc, .rar, .avi, and .mp3 files on drives C, D, E, and F. W32.HLLO.Rozak is written in a high-level language. It needs the Neh.dll file, which is a exact copy of itself. When it is executed, it searches drives C, D, E, and F for files that have the following extensions: .exe, .mpg, .mpg4, .zip, .doc, .rar, .avi, and .mp3. It then copies itself as Neh.dll and overwrites the files. The overwritten program files are not repairable.

W32.Pixo (Win32 Worm): This is a Visual Basic worm that copies itself to the \Windows\System folder and to any disk that is in the A drive. When it is executed, this worm copies itself to the %System% folder using the same name as was used by the file that was just executed. Then it adds the value, "Rundll32.exe C:\Windows\System\PIX-61081.exe," to the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

W32.Taripox@mm (Aliases: I-Worm.Taripox.b, W32/Taripox.b, Carrytone) (Win32 Worm): This is a UPX-packed mass-mailing worm that uses a new replication technique. Serving as a SMTP proxy on a local computer, it injects itself into the outgoing email messages. When it is executed, W32.Taripox@mm copies itself as \%Windows%\Mmoplib.exe. It adds the value, mmopl "\%Windows%\MMOPLIB.EXE" to the registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

to enable itself to run when Windows starts. Next the worm remaps the SMTP server of the Default Mail Account to the local host IP address (127.0.0.1). To do this, the worm modifies the following file:

\%Windows%\system32\drivers\etc\HOSTS *NOTE: Because a different HOSTS file is used by Windows 95/98/Me for the locally predefined host name resolutions, the worm may not replicate under these operating systems.*

Running as an SMTP proxy, W32.Taripox@mm listens on port 25 (SMTP port). Whenever an e-mail client attempts to establish a connection with the SMTP server, it creates a stream socket for the internetwork TCP/IP connection and establishes a connection to that socket using port 25 and the IP address of the SMTP server. This IP address will not be resolved for the host since it is already remapped by the worm. This results in establishing a connection with the worm. The e-mail client starts to communicate with W32.Taripox@mm as it would with the real SMTP server. The worm examines and passes the communication streams to and from the SMTP server. When the e-mail program transmits the "DATA" command to initiate the e-mail transmission, W32.Taripox@mm intercepts the DATA stream and sends different data: the original message with the injected viral attachment. The worm preserves the sender, the recipient, and the message body of the original e-mail message. However, if the original attachment is smaller than 6 KB, the worm adds its own viral body. The file name of the viral MIME-encoded attachment is the recipient's name with the ".doc.pif" string appended. The worm places "taricone" as the viral attachment name so that some e-mail clients will display this name instead. The viral "taricone" file is also attached to an e-mail if the original message contains no attachments. If the original attachment is larger than 6 KB, the worm substitutes it with the MIME-encoded viral body, retaining the original file name as a name of the viral attachment. If the original attachment has an extension other than .exe, the file name of the viral attachment is the original attachment file name with the ".exe" extension appended to it. To hide its activity as much as possible, the worm keeps a five-member queue (FIFO) in the value, MRU, of the registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Media Optimization Library

Before the DATA stream interception, the worm checks whether the recipient name is among the members of this queue. If it is not, the virus sends itself to that recipient and add the recipient's name to the queue, pushing out the last member from the queue. If the recipient is found in the queue, the virus will not submit itself to that person again.

WM97/Ded-T (Word 97 Macro Virus): This is a polymorphic member of the WM97/Ded family. It may delete the Word Normal.dot file.

WM97/Panggil-C (Word 97 Macro Virus): WM97/Panggil-C will set the Word application user information as follows:

- UserName: Grunge-X Include in
- UserInitials: Grunge-X
- UserAddress: Grunge-X@usa.net

It can also set a document password of "GRUNGE ." If the user accesses Tools|Macro, the virus will use the Office Assistant to display the message:

"GRUNGE Is Block Your System
System Is Disabled By (Grunge)
You Can't Open VBMacro Code On this time, because the System is Busy please check on your administrator system."

The virus can also change the Word application caption to read either "Include Grunge-X, please wait... " or "Keep to Smile." On Mondays and Fridays, it will display the following message when Word exits:

"The Sun Is Gone But I Have I Light (1967-1994)."

WM97/Panggil-C creates a directory called OSGrunge under the Windows directory in which it keeps an infection log in Grunge1.ini. The virus also creates the non-viral file Engine.dll in the Word application directory.

WORM_MALDAL.I (Alias: DAZ2ME Worm) (Worm): This worm has been reported in the wild. It is an Aspack-compressed mass-mailing worm compiled using Visual Basic 5.0. It uses Microsoft Outlook to propagate itself by using random names taken from directory names found in the infected user's machine. It arrives as an e-mail message with a pedefined set of subject headers it uses to catch the interest of the recipients. The body text of the e-mail is likely to be blank and the filename of the attachment is most likely to be PROGRAM.EXE. The worm can extract e-mail addresses from web pages on the hard drive as well as from the Microsoft Outlook address book. When first run W32/Maldal-I will set the registry key, HKLM\Shadup. When next run it will display a box with a black background and red text stating:

"Sorry you have not registered
Please contact us"

along with some phone numbers, e-mail addresses and instructions on how to subscribe. It will then set the registry key, HKLM\e5zemha. The worm will create several entries in the registry Run key all pointing to copies of itself scattered over the harddisk, although it may not actually create the associated files. Five minutes after being run, the worm may display a black background with the following text in red letters:

ZaCker Is N YoUr MaChiNe

WORM_MONKEY.B (Aliases: MONKEY.B, MONKEY, I-Worm.Monkey) (Worm): This is a destructive, UPX-compressed, and Visual Basic compiled, mass-mailing worm. Upon execution, it drops files and creates an entry in the AutoRun key of the system registry. It uses Microsoft Outlook to propagate copies of itself via e-mail to all e-mail addresses listed in the infected user's address book. It can delete system files.

WORM_VALCARD.A (Aliases: VALCARD.A, I-Worm.Valcard) (Worm): This is a mass-mailing worm that drops files in a system. It sends an e-mail with a file attachment, VALENTINECARD.EXE, to the list of recipients found in the Microsoft Outlook address book.

WORM_YAHA.A (Aliases: W32/Yaha@mm, YAHA.A) (Worm): This mass-mailing worm is compiled in Visual C++. It arrives in an infected e-mail with itself as an attachment, called "valentin.scr." Upon execution, it drops the following two hidden copies of itself in the recycle bin, c:\recycled:

- msmdm.exe
- msscra.exe

WORM_YARNER.A (Aliases: YARNER.A, YAWSETUP, W32.Yarner.A@mm) (Worm): Upon execution, this mass-mailing worm, compiled in Delphi, drops files and creates an entry in the AutoRun key of the system registry. It propagates via Microsoft Outlook by sending itself out to all e-mail addresses listed in the address book of the infected user.

WORM_YARNER.B (Alias: WORM_YARNER.GEN) (Worm): This worm is a recompiled version of the original worm, WORM_YARNER.A and has similar characteristics. Upon execution, this mass-mailing worm, compiled in Delphi, drops files and creates an entry in the AutoRun key of the system registry. It propagates via Microsoft Outlook by sending itself to all e-mail addresses listed in the address book of the infected user.

XM.Momac.A (Excel Macro Virus): This is an Excel macro virus that spreads from an infected workbook to all currently open workbooks. Based on the fact that the variable names of the source for this virus are all in French, it appears that it may have French origins. The name of the virus is derived from the macro module that it resides in, OMMacro.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table starts with Trojans discussed in CyberNotes #2001-01, and items will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. *Note: At times, Trojans may contain names or content that may be considered offensive.*

Trojan	Version	CyberNotes Issue #
APStrojan.sl	N/A	CyberNotes-2002-03
Backdoor.EggHead	**N/A**	**Current Issue**
Backdoor.IISCrack.dll	**N/A**	**Current Issue**
Backdoor.NetDevil	**N/A**	**Current Issue**
Backdoor.Palukka	N/A	CyberNotes-2002-01
Backdoor.Subwoofer	**N/A**	**Current Issue**
Backdoor.Surgeon	**N/A**	**Current Issue**
Backdoor.Systsec	**N/A**	**Current Issue**
BackDoor-AAB	N/A	CyberNotes-2002-02
BackDoor-FB.svr.gen	N/A	CyberNotes-2002-03
BKDR_SMALLFEG.A	**N/A**	**Current Issue**
DlDer	N/A	CyberNotes-2002-01
DoS-Winlock	N/A	CyberNotes-2002-03
Hacktool.IPStealer	N/A	CyberNotes-2002-02
Irc-Smallfeg	N/A	CyberNotes-2002-03
JS/Seeker-E	N/A	CyberNotes-2002-01
JS_EXCEPTION.GEN	N/A	CyberNotes-2002-01
SecHole.Trojan	N/A	CyberNotes-2002-01
Troj/Download-A	N/A	CyberNotes-2002-01
Troj/Msstake-A	N/A	CyberNotes-2002-03
Troj/Optix-03-C	N/A	CyberNotes-2002-01
Troj/Sub7-21-I	N/A	CyberNotes-2002-01
Troj/WebDL-E	N/A	CyberNotes-2002-01
TROJ_CYN12.B	N/A	CyberNotes-2002-02
TROJ_DANSCHL.A	N/A	CyberNotes-2002-01
TROJ_DSNX.A	N/A	CyberNotes-2002-03

Trojan	Version	CyberNotes Issue #
TROJ_FRAG.CLI.A	N/A	CyberNotes-2002-02
TROJ_ICONLIB.A	N/A	CyberNotes-2002-03
TROJ_SMALLFEG.DR	**N/A**	**Current Issue**
Trojan.Badcon	N/A	CyberNotes-2002-02
Trojan.StartPage	N/A	CyberNotes-2002-02
Trojan.Suffer	N/A	CyberNotes-2002-02
VBS.Gascript	**N/A**	**Current Issue**
VBS_THEGAME.A	N/A	CyberNotes-2002-03

Backdoor.EggHead: This is a backdoor Trojan horse program that uses a freeware IRC bot as its core component. This backdoor works only under Windows NT/2000/XP. Once activated, this backdoor gives a third party unrestricted access to the client's computer.

Backdoor.IISCrack.dll: This backdoor Trojan is a Dynamic Link Library (DLL) that is used to attack and exploit IIS servers. If the attack is successful, then the attacker will have gained System level access to the server. For this backdoor to work, the attacker must be able to copy it to the server's scripts directory. Once there, the attacker just uploads the DLL using his Web browser (for example URL/scripts/backdoor.dll), and uses the DLL to give commands to the system.

Backdoor.NetDevil: Backdoor.NetDevil allows a malicious user to remotely control an infected computer. When Backdoor.NetDevil is run, it copies itself to the %System% folder. The file name that it uses may vary, because the malicious user who creates this Backdoor Trojan can choose any desired file name. It adds a value that refers to the dropped file to one of the following registry keys:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

When the malicious user creates the BackDoor.NetDevil server file, there are many functions that can be added. It can be programmed to:

- Display a fake error message to conceal its true nature
- Choose the ports that are used by the backdoor to communicate with the malicious user. By default, it uses port 901 for direct control, port 902 for communicating logged key strokes, and port 903 for file transfer
- Use different notification methods to send information to the malicious user about the compromised computer
- Attempt to kill running firewall and antivirus processes

If Backdoor.NetDevil is run, it allows the malicious user to remotely take control over the compromised computer, and can include:

- Full control over the file system
- Upload to and download from the host computer
- Run files of the malicious user's choice
- Kill running processes
- Display messages
- View the screen
- Log key strokes
- Annoying actions, such as manipulate the mouse, open and close the CD-ROM drive, turn the monitor on and off, and so on.

Backdoor.Subwoofer: When Backdoor.Subwoofer is run, it copies itself to the %System% folder as:

- %System%\Scheduler.exe
- %System%\Channel.src

and it drops the file %System%\Tweak.dll. To enable itself to run at startup, it adds the value, Tweak UI "RunDLL32 tweakUI.DLL, TWEAKUI /tweakmeup" to the registry key:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

and the value, Scheduling Agent "Scheduler.exe" to the registry key:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

If Backdoor.Subwoofer is run, it allows the malicious user to remotely take control over the compromised computer.

Backdoor.Surgeon (Alias: Backdoor.Infector): Backdoor.Surgeon allows a malicious user to remotely control an infected computer. When Backdoor.Surgeon is run, the malicious user can merge this backdoor Trojan with a valid program so that the actual Trojan goes unnoticed when it is run. It copies itself to the %Windows% folder. The file name that it uses may vary, because the malicious user who creates this backdoor Trojan can choose any desired file name. To be run at system startup, this backdoor Trojan can modify one of the following startup locations: It can add a value that refers to the dropped file to one of the following registry keys:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

It can start from the "Run=" line in the %Windows%\Win.ini file. It can start from the "Shell=" line in the %Windows%\System.ini file. This Trojan can be configured to use ICQ or IRC to notify the malicious user that it successfully compromised a system. Backdoor.Surgeon allows the malicious user to take control of the compromised system by opening a port. The malicious user who creates the backdoor can configure the port. By default, it uses port 35000. If Backdoor.Surgeon is run, it allows the malicious user to remotely take control over the compromised computer.

Backdoor.Systsec: This is a backdoor Trojan horse. It listens on port 1034 and allows unauthorized access to an infected computer. It sets itself up to run automatically when Windows restarts. If more than one instance of Backdoor.Systsec is run, the new one opens the next higher numbered port. To enable itself to run at startup, it adds the value:

SystSecure32 SystSecure32.exe

to the following registry key:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\

BKDR_SMALLFEG.A (Alias: SMALLFEG.A): This backdoor Trojan is dropped by TROJ_SMALLFEG.DR, and executes as a service process. It attempts to establish a connection to several remote IRC servers, all with the domain name "undernet.org." It attacks IRC servers by sending foul messages.

TROJ_SMALLFEG.DR (Alias: SMALLFEG.DR, Irc-Smallfeg): Upon execution, this dropper Trojan drops the files “svchost.exe” and “jupe.dll” in the %Windows%\Cache directory. It modifies the registry to allow the dropped file “svchost.exe” (detected as BKDR_SMALLFEG.A) to execute at every Windows startup.

VBS.Gascript: This Trojan that displays a message in Notepad and changes the Internet Explorer home page. When VBS.Gascript is run, it copies itself to C:\Windows\Camila.vbs. and adds the value, ‘Kuasanagui wscript.exe C:\WINDOWS\camila.vbs %’ to the registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that it runs when you start Windows. It also creates the file C:\Windows\El microbito.txt and then sets the Internet Explorer home page to the virus writer's homepage by changing the following values:

- Start Page
- Window title

in the registry key:

HKEY_USERS\.DEFAULT\SOFTWARE\Microsoft\Internet Explorer\Main